International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

Authentication in Wireless Sensor Networks

Dr. K. Nachimuthu M.C. A, M. Phil, Ph.D[1], A. Pushpavalli M. SC., B. E d.,[2]
[1]*Research Advisor,Jairam's Arts and Science College, Karur, Tamilnadu, India*
[2] *Research Scholar,Jairam's Arts and Science College, Karur, Tamilnadu, India*

Abstract: Wireless Sensor Networking (WSNs) is a region of incredible enthusiasm to both scholarly community and industry. WSNs raise countless, mechanical, logical, non military personnel and business applications to another level, permitting financially savvy detecting, particularly where human perception or conventional sensors would be unwanted, wasteful, costly, or risky. Indeed, even from their soonest applications, sensor systems have been focused for assault by foes with enthusiasm for blocking the information being sent, or in lessening the capacity of the system to do its main goal. There are a great deal of conceivable assaults against WSNs, which have distinctive goals, are performed at various levels, and result in various outcomes. Remote sensors have restricted vitality and computational capacities, making numerous conventional security procedures troublesome or difficult to be used. Likewise, they are regularly sent in open unattended regions, permitting physical assaults, for example, sticking, hub catch and altering. Then again, consistent assaults incorporate the HELLO flooding assault, the Sybil assault, the sinkhole assault, the wormhole assault, the blackhole assault, and the Distributed Denial of Service (DDoS) assault. Noteworthy research exertion is done to address every one of these issues. Wireless Sensor Networking (WSNs) is a developing field of research that presents analysts with testing objectives under tight outline imperatives. The requirement for inventive and imaginative security conventions is clear, since current security instruments are excessively asset serious as far as power, memory and preparing capacities of sensor organize hubs.

Keywords: Wireless Sensor Network, DSN, Node Capture, Denial of Service, Collisions, MAC layer

I. INTRODUCTION

A Wireless Sensor Network (WSN) is defined as a large set of tiny sensor nodes (the number varies from few to several hundreds or thousands) with sensing, computational and communication capabilities. Like many advanced technologies, the origin of WSNs is found in military and heavy industrial applications. The Sound Surveillance System (SOSUS) [1], developed by the United States Military in the 1950s, during the Cold War, to detect and track Soviet submarines, is the ancestor of modern WSNs.

Later, in the early 1980s, the United States Defense Advanced Research Projects Agency (DARPA) launched the Distributed Sensor Networks (DSN) program to examine the potential benefits in implementing distributed wireless sensor networks, which was followed by the Sensor Information Technology (SensIT) [2] program that provided the present sensor networks with new capabilities, such as ad hoc networking, dynamic querying and tasking, reprogramming and multi-tasking.

Major advances in microelectromechanical systems (MEMS), CMOS-based semiconductor devices, networking protocols (IEEE 802.15.4 standard [3] or ZigBee) and energy storage technologies, dramatically reduced the high deployment and mainly maintenance cost and leveraged the widespread adoption of WSNs into a broader range of applications, including home automation, smart environments, continuous medical monitoring systems, environmental control and many others.

In short, we can presume that future WSNs will form the building blocks of the Internet of Things [4] , changing our everyday life in unprecedented and unanticipated ways.

A. Security Issues

A Wireless Sensor Network (WSN) may share some similarities to a typical computer network, but due to its power, computation, storage and communication constraints and the high dependency on the physical environment of deployment, the existing security approaches cannot be directly affiliated.

Consequently, in order to implement an efficient security scheme:

1) It is essential to limit the code size of the security algorithm,
2) When implementing a cryptographic function or protocol, the energy impact on the whole network must be considered,
3) Communication in most cases is unreliable due to the broadcast nature of radio transmission and iv) sensor nodes may be physically destroyed or compromised.

B. Security requirements of WSN

According to [5], the security requirements of a wireless sensor network can be classified as follows:

1) *Availability:* The service that is offered by the whole WSN, by a part of it or by a single sensor is available, whenever it is required. This means that the security algorithm should not add any computation and/or communication overhead to sensor nodes and force them to run out of power, becoming this way unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.
2) *Authentication:* As in traditional networks, authentication is necessary to ensure the receiver that any data used in decision-making processes, originate from the correct source. Authentication ensures the authenticity of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false or bogus packets. Node's authentication verifies the identity of the senders and receivers. Node's authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless transmission and the unattended nature of sensor networks, it is extremely challenging to ensure authentication. Authentication will be discussed further in the following sections.
3) *Confidentiality:* In many applications (e.g. military or industrial), data collected by the sensor nodes may be extremely sensitive. Therefore, data confidentiality is the most important issue in WSN security. In addition, information about the sensors, such as identities and public keys, should also be protected against traffic analysis attacks. The standard approach for keeping sensitive data secret is through encryption.
4) *Integrity:* Adversaries can also alter and fabricate the data by adding fragments or manipulating data within packets and then send them to the indented receiver. Information damage can even occur without the presence of malicious nodes, due to the harsh communication environment
5) *Data freshness/Nonreplay:* Adrian Perrig et al. [6] define data freshness to mean recent data and mechanisms ensuring that no adversary replayed old messages. To solve this issue, nonces such as timestamps can be added to the communication protocol.

II. ATTACKS AGAINST WIRELESS SENSOR NETWORK

An *attack* can be defined as an attempt to gain unauthorized access to a service, a resource or information or to damage any normal operation. In other words, it is an attempt to compromise availability, confidentiality or the integrity of a system or to spoof identities.

A. Classification of Attacks

Attacks can be classified into different categories according to certain criteria. A first distinction can be made between mote-class attacks and laptop-class attacks. Mote-class attackers have access to a few sensor nodes with similar capabilities as the sensors of the. These attackers might only be able to jam the radio link in their immediate vicinity. Also in mote-class attacks evil nodes might intercept forwarded information and route some messages to specific destinations (blackhole attack).

On the other hand, laptop-class attackers may have devices with greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna. In this case, the attacker has an advantage and he is able to compromise the entire sensor network, not just a few nodes.

Another distinction may be between *active* and *passive* attacks. Active attacks attempt to alter or destroy the data packets being transmitted, disrupting this way the normal function of the network and violating its integrity. A passive attack does not disrupt the function of the network, as the attacker eavesdrops the data without altering them. Since the network itself does not get affected, the detection of a passive attack is not a trivial task.

Attacks can be further classified into *external* and *internal*, depending on where the malicious nodes belong. External attacks are carried out by nodes that do not belong to the network and may range from passive eavesdropping, as well as injecting false data to the network, to consume resources and raise Denial of Service (DoS). Internal attacks are carried out by compromised nodes of the network. Since the attackers have become part of the network as legitimate nodes, internal attacks are more severe and harder to detect in relation with external attacks.

B. Physical Attack

This attack is also known as node capture [7]. In this type of attack, attackers gain full control over some sensor nodes through direct physical access. As the cost of sensor nodes must be kept as cheap as possible for WSN, sensor nodes with tamper proofing features are impractical.

This is why sensor nodes are susceptible to being physically accessed. Physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.
Designing sensor nodes with hardware platform of up to date embedded system security can improve the physical level security. Moreover, monitoring sensor nodes for unusual length of inactivity period and revocation of suspicious node's authentication token are necessary steps which should be taken for securing WSN against physical or node capture attacks.

C. Denial of Service Threats in WSNs

In literature, as Denial of Service (DoS) attack, is defined any condition that can diminish or even eliminate a network 's capacity to perform as expected, including hardware failures, bugs, resource exhaustion, malicious attacks and environmental conditions.

D. Physical layer attacks

There are two well-known attacks against the physical layer of a WSN.
Jamming interferes with the radio frequencies the nodes are using. Only a few jamming nodes can put a considerable amount of legitimate nodes out of order. If the adversary blocks the entire network, effective and complete DoS results. However, large networks are hard to block in their entirety.
Nodes may fall victims to physical *tampering*, especially if they are part of a network that covers a vast area. A tampering attacker may damage a sensor, replace the entire node or part of its hardware or even electronically interrogate the nodes to gain access to sensitive information, such as shared cryptographic keys and how to access higher communication layers.

E. Link layer Attacks

Collisions, unfairness or exhaustion attacks can be launched against the data link layer of a sensor network. Collisions are a type of link layer jamming. If an attacker can corrupt an octet of transmission such that a checksum mismatch occurs, then the entire packet can be disrupted. Corrupted ACK messages usually lead to costly exponential back-off in some MAC protocols. A compromised node may also intentionally deny access to a channel, whilst expending less energy required by full-time jamming of the channel.
Unfairness is a weaker form of DoS that is done by abusing MAC priority schemes. Such an attack usually leads to loss of real-time deadlines and hence degradation of service.
Exhaustion of battery resources may occur when naive link layer implementations attempt repeated retransmission even after unusually late collisions. A variation of this attack is when a self sacrificing node continuously asks for access to a channel, forcing its neighbors to respond with a Clear To Send (CTS) message.

F. Network Layer Attacks

Wood and Stankovic [8] inform us that neglect and greed, homing, misdirection, authorization, probing, black holes and monitoring are ossible routing layer attacks. Karlof and Wagner [9] give specific names to these attacks and describe them in detail.
Spoofed, altered or replayed routing information is the most direct attack. By spoofing, altering or replaying routing information the attacker can complicate the network by creating routing loops, attracting or repelling traffic, generating false error messages, shortening or extending source routes or partitioning the network.

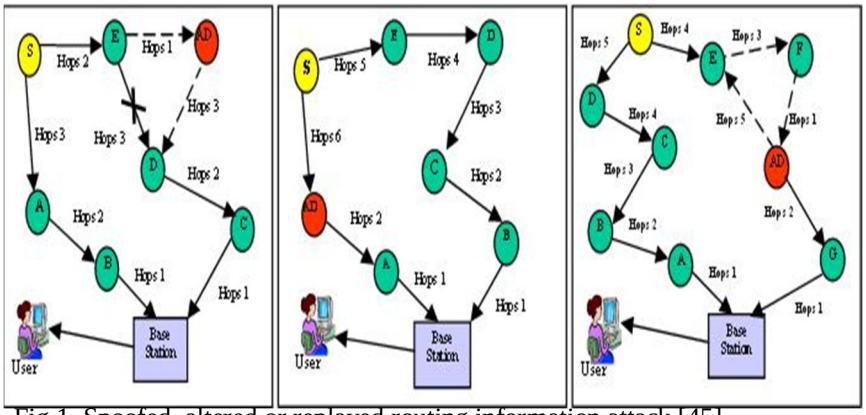

Fig 1. Spoofed, altered or replayed routing information attack [45]

In Selective Forwarding the adversary includes him/herself in a data flow path of interest. Then the attacker may choose not to forward certain packets and drop them causing a sort of black hole. A variation of this attack is when the adversary only drops packets coming from a specific source whilst reliably forwarding other packets. Such attacks are much harder to detect than black hole attacks.

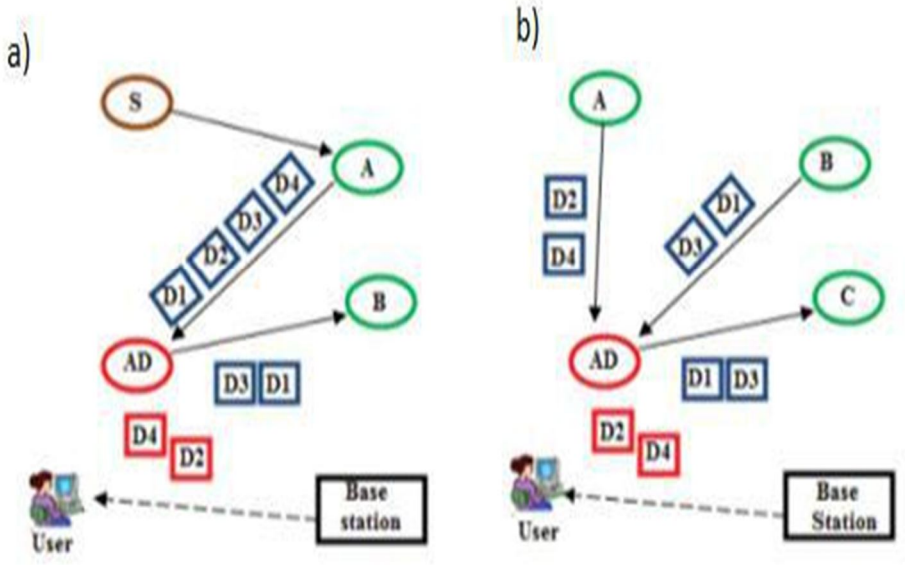

Fig.2 Selective forwarding attack
(a) adversary drops selected packets of a node (b) adversary drops all packets from a selected node [10]

The goal of a sinkhole attack is to lure traffic to a malicious part of the network. Such attacks are usually the launching block for other attacks such as selective forwarding. Sinkholes work by making a compromised node attractive to its neighbors. This is done by advertising high quality routes, i.e. low latency routes. Fooled neighbors will then forward all their data destined to the base station to the lying node. Sensor networks are susceptible to these attacks due to their multi-hop nature and the specialized communication patterns they use.

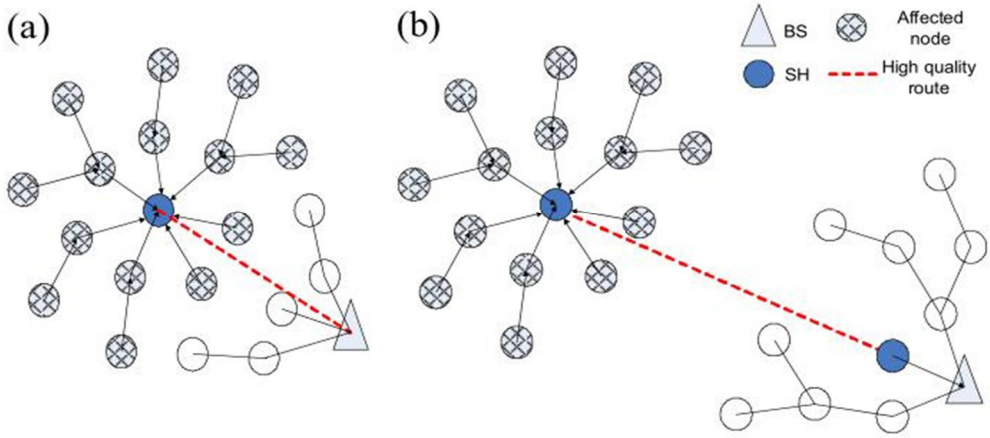

Fig 3. Two examples of sinkhole attack in wireless sensor networks.
(a) Using an artificial high quality route; (b) Using a wormhole. [11]

The Sybil attack targets fault tolerant schemes such as distributed storage, dispersity, multipath routing and topology maintenance. This is done by having a malicious node present multiple identities to the network. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at the same time.

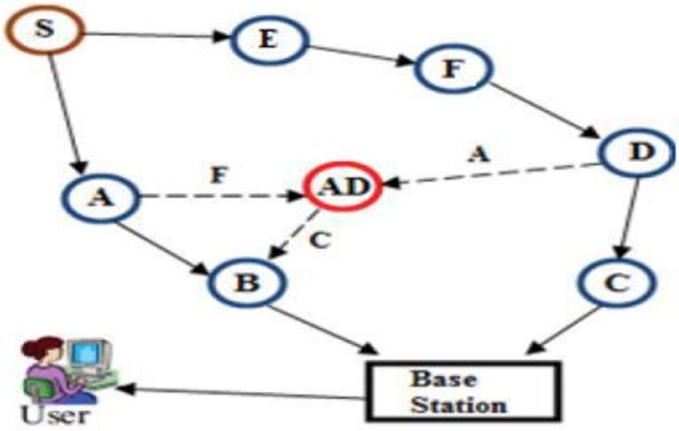

Fig 4. Sybil Attack

In wormhole attacks the adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. The simplest occurrence of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbors, leading to quick exhaustion of their energy resources. An attacker close to the base station can completely disrupt routing by creating well positioned wormholes that convince nodes multiple hops from the base station that they are only a couple of hops away through the wormhole. When this attack is coupled with selective forwarding and Sybil attack, it is very difficult to detect.

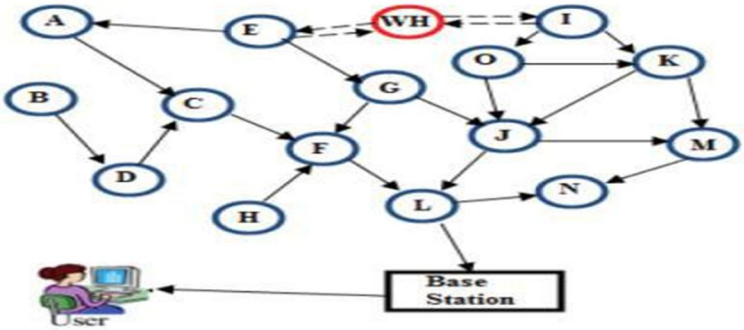

Fig 5. Wormhole Attack

1) *Hello flood attacks:* In many routing protocols, nodes broadcast hello messages to announce their presence to their neighbors. A node receiving such a message can assume that the node that sent the message is within its range. An attacker with a high powered antenna can convince every node in the network that he is their neighbor. If the attacker also advertises a high quality route it can get every node to forward data to it. Nodes at a large distance from the attacker will be sending their messages into oblivion leaving the network in a state of confusion. This attack can also be thought of as a type of broadcast wormhole. Routing protocols dependant on localized information are extremely vulnerable to such attacks.

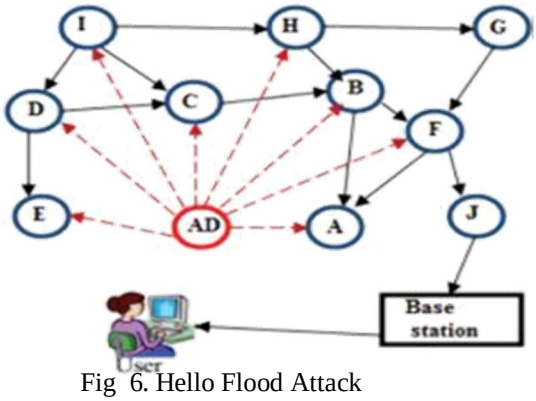

Fig 6. Hello Flood Attack

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

2) *Acknowledgement Spoofing*: Protocols that choose the next hop based on reliability issues are susceptible to acknowledgments spoofing. Here the attacker spoofs acknowledgement convincing the sender that a weak link may be strong or a dead node is alive. This results in packets being lost when travelling along such links.

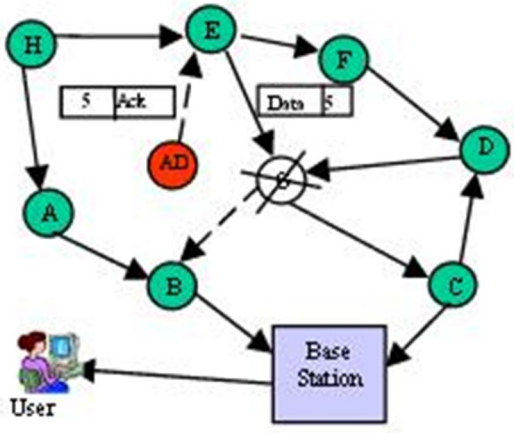

Fig 7. Acknowledgment Spoofing Attack

3) *Application Layer Attacks: Finally, the application layer can be attacked via overwhelm attack, path-based DOS attack and deluge (reprogram) attack.*

In *overwhelm attack*, an attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to sink. This attack consumes network bandwidth and drains node energy. We can mitigate this attack by carefully tuning sensors so that only the specifically desired stimulus, such as vehicular movement, as opposed to any movement, triggers them. Rate-limiting and efficient data-aggregation algorithms can also reduce these attacks' effects.

based DOS attack involves injecting spurious or replayed packets into the network at leaf nodes. This attack can starve the network of legitimate traffic, because it consumes resources on the path to the sink, thus preventing other nodes from sending data to the sink. Combining packet authentication and anti replay protection prevents these attacks.

Finally, in deluge (reprogram) attack, network-programming system let you remotely reprogram nodes in deployed networks. If the reprogramming process isn't secure, an intruder can hijack this process and take control of large portions of a network. Authentication streams may be used to secure the reprogramming process.

III. COUNTERMEASURES AGAINST DOS ATTACKS

Since denial-of-service attacks are so common, effective defenses must be available to combat them. One strategy in defending against the classic jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion. Wood and Stankovic [8] describe a two-phase approach where the nodes along the perimeter of the jammed region report their status to their neighbors who then collaboratively define the jammed region and simply route around it.

To handle jamming at the MAC layer, nodes might utilize a MAC admission control that is rate limiting. This would allow the network to ignore those requests designed to exhaust the power reserves of a node. This, however, is not foolproof as the network must be able to handle any legitimately large traffic volumes.

Overcoming rogue sensors that intentionally misroute messages can be done at the cost of redundancy. In this case, a sending node can send the message along multiple paths in an effort to increase the likelihood that the message will ultimately arrive at its destination. This has the advantage of effectively dealing with nodes that may not be malicious, but rather may have simply failed as it does not rely on a single node to route its messages.

To overcome the transport layer flooding DoS attack, Aura, Nikander, and Leiwo[12] suggest using client puzzles in an effort to discern a node's commitment to making the connection, by utilizing some of its own resources. Table 1 list the layers of a typical sensor network and describe each layer's vulnerabilities and defences.

TABLE 1
DENIAL-OF-SERVICE ATTACKS AND DEFENCES BY PROTOCOL LAYER

Protocol Layer	Attacks	Defences
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle ,region mapping mode change
	Node tampering or destruction	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Neglect and greed	Redundancy, probing
	Homing	Encryption, Dummy Packets
	Misdirection	Egress filtering, authorization, monitoring
	Spoofing, replaying, or altering routing-control traffic or clustering messages	Authentication and antireplay protection Secure cluster formation
	Selective forwarding attack	Multipath routing
	Sinkholes	Geographic routing Protocols
	Black holes	Authorization, monitoring, Redundancy
	Sybil	Code attestation, resource testing, location verification, key-based Authentication
	Wormhole	Packet leashes, monitoring
	Hello floods	Pairwise authentication, Geographic routing
Transport	Flooding	Client puzzles
	Desynchronization	Authentication
Application	Overwhelming sensors	Sensor tuning
	Path-based DoS	Authentication and antireplay protection
	Deluge (reprogramming) attack	Authentication and antireplay protection, Authentication streams

IV. CONCLUSION

Authentication is a very crucial security requirement in WSNs, as sensor nodes are often deployed in unattended environment and thereby vulnerable to attacks. Authentication ensures a receiver that data, mobile code or control data such as route updates, location information and key management messages originate from the correct source. If a strong authentication mechanism is not included, then an adversary can often spoof others identity, generate fake data packets and force sensor node to relay those packets, draining their energy. A fake message can cause sensor nodes to accept and transfer wrong information which in turn makes sensor nodes prone to various attacks.

Different authentication issues stem from the type of node deployment. In case of a static deployment, the nodes never move. Such nodes are vulnerable to replay attacks and node capture, as the nodes are easily traceable. On the other hand, in case of a dynamic deployment, issues such as re-authentication of mobile nodes, untraceability of nodes' movement and message integrity may arise.

To secure the communication over WSN, we need an authentication method which can ensure that unauthorized nodes cannot join the network as well as they cannot transmit any data over the network.

REFERENCES

[1] E. C. Whitman, "Sosus, the Secret Weapon of undersea surveillance," Undersea Warfare - The official website of the U.S. Submarine Force, 2005. [Online]. Available:http://www.navy.mil/navydata/cno/n87/usw/issue_25/sosus2.htm.

[2] S. Kumar and D. Sepherd, "SensIT: Sensor Information Technology for the Warfighter," Proc. 4th Int. Conf. on Information Fusion - isif.org, 2001.

[3] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in Proceedings of the 2004 ACM workshop on Wireless security - WiSe '04, Philadelphia, PA, USA, 2004.

[4] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," Computer Networks, 31 May 2010.

[5] J. Walters, Z. Liang, W. Shi and V. Chaudhary, "Chapter 16. Wireless Sensor Network Security:A Survey," in Security in distributed, grid, mobile, and pervasive computing, Auerbach Publications, CRC Press, 2007, pp. 367-409.

[6] A. Perrig, R. Szewczyk, J. Tygar, V. Wen and D. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, Volume 8, Issue 5, pp. 521-534, 2002.

[7] A. Becher, Z. Benenson and M. Dornseif, "Tampering with motes: real-world physical attacks on wireless sensor networks," in Proceedings of the Third international conference on Security in Pervasive Computing, SPC'06, York, UK, 2006.

[8] A. Wood and J. Stankovic, "Denial of service in sensor networks," IEEE Computer, Volume 35, Issue 10, pp. 54-62, October 2002.

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, Volume 1, Issue 2-3, pp. 293-315, 2003.

[10] S. Amara, R. Beghdad and M. Oussalah, "Securing Wireless Sensor Networks: A Survey," EDPACS: The EDP Audit, Control, and Security Newsletter, Volume 47, Issue 2, pp. 6 - 29, 4 February 2013.

[11] E. Ngai, J. Liu and M. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," in IEEE International Conference on Communications, Istanbul, 2006.

[12] T. Aura, P. Nikander and J. Leiwo, "DOS-Resistant Authentication with Client Puzzles," in Revised Papers of 8th International Workshop on Security Protocols, Cambridge, UK, 2001.